Jurnal Asiimetrik: Jurnal Ilmiah Rekayasa Dan Inovasi
Terakreditasi **"Peringkat 4"** oleh Kemenristek/BRIN, Nomor SK: 200/M/KPT/2020
Volume 5 Nomor 1 Tahun 2023, Januari 2023, Halaman 93-100
Website : http://journal.univpancasila.ac.id/index.php/asiimetrik/

p-ISSN 2655-1861
e-ISSN 2716-2923

Peningkatan Keamanan pada *Simple Network Time Protocol* (SNTP) untuk Mendeteksi *Cybercrime* di dalam Aktivitas Jaringan

Improved Security on Simple Network Time Protocol (NTP) to Detect Cybercrime in Network Activity

Kotim Subandi*, Victor Ilyas Sugara dan Adriana Sari Aryani
Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Pakuan, Jl. Pakuan, RT.02/RW.06, Bogor, Jawa Barat 16129, Indonesia

Informasi artikel:

Diterima:
16/11/2022
Direvisi:
27/11/2022
Disetujui:
01/12/2022

Abstract

Today's cybercrime methods are extremely diverse. The methods employed by attackers are becoming more diverse and intricate. Malicious software, commonly referred to as malware, is utilized in these various attacks. Malware threats and their propagation can be accomplished in several different ways. Good governance facilitates prevention via migration, assisting the security team and network infrastructure IT. This paper discusses efforts to enhance the security of the Simple Network Time Protocol (SNTP) to detect cybercrime on the network. Based on the results of the conducted experiments, we determined that by updating the Simple Network Time Protocol, implementing the client-server antivirus, and scanning every client connected to the local network or centrally, we could detect the types of attacks that frequently occur on the network system, thereby protecting all client computers from malware, viruses, worms, and Trojan horses. Based on the antivirus migration data, the employed research method can find information on cybercrimes that involve malware that enters the network and is successfully cleaned or quarantined before being automatically blocked.

***Keywords**: security, network, protocol, cybercrime.*

***SDGs*:**

Abstrak

Modus kejahatan di dunia maya saat ini sangat beragam. Cara yang digunakan oleh penyerang semakin beragam dan kompleks. Berbagai serangan tersebut melibatkan *malicious software* atau yang biasa disebut *malware* yang merupakan suatu program jahat. Ancaman *malware* dan penyebarannya bisa melalui berbagai cara. Dengan cara migrasi dapat melakukan pencegahan dengan tata kelola yang baik, sehingga dapat membantuan tim keamanan dan IT Infrastruktur Jaringan. Tulisan ini membahas tentang upaya peningkatan keamanan pada *Simple Network Time Protocol* (SNTP) untuk mendeteksi *cybercrime* di dalam aktivitas jaringan. Berdasarkan hasil percobaan yang dilakukan, bahwa dengan memperbaharui *Simple Network Time Protocol* dan mengimplementasi *antivirus client server* serta melakukan *scan* di setiap *client* yang terhubung jaringan lokal maupun secara terpusat dapat mendeteksi jenis serangan yang sering terjadi pada sistem jaringan, hingga memberikan proteksi seluruh komputer *client* dari segala serangan seperti *malware, virus, worm, Trojan*. Berdasarkan data migrasi *antivirus* dengan metode penelitian yang dilakukan dapat menemukan data kejahatan *cybercrime* berupa *malware* yang masuk ke ruang lingkup jaringan berhasil *cleaned* atau *quarantine* hingga *blocked* secara otomatis.

Kata Kunci: keamanan, jaringan, protokol, *cybercrime*.

*Penulis Korespondensi. Tel: -; Handphone: +62 815 1339 4498
email : kotim.subandi@unpak.ac.id

1. PENDAHULUAN

Di era sekarang ini teknologi informasi dan komputasi telah berkembang pesat sehingga kejahatan dunia maya meningkat secara drastis karena pandemi, penjahat dunia maya kini juga menargetkan orang, bukan hanya sistem yang ada di dalam perusahaan saja, dengan terintegrasi dengan teknologi informasi serta layanan sentris komunikasi di jaringan (Adnan, Ikhwan dan Rahmawati, 2018). Arsitektur komputasi dan sifat akses dengan jaringan ini mengubah secara drastis format model penyampaian informasi .

Pandemi Covid yang sudah terjadi beberapa tahun belakangan ini meng-haruskan beberapa karyawan bekerja dari rumah *Work From Home* (WFH). Hal ini mengakibatkan serangan *ransomware attack* meningkat di ikuti juga dengan penjahat dunia maya yang memanfaatkan perubahan cara bekerja pada saat pandemi ini, sehingga keamanan jaringan dari tindak kejahatan *(cyber security*) sangat penting aktivitas bekerja jarak jauh (BSSN, 2022).

Modus kejahatan di dunia *cyber* saat ini sangat beragam. Cara yang digunakan oleh penyerang semakin beragam dan kompleks. Berbagai serangan tersebut melibatkan *malicious software* atau yang biasa disebut *malware* yang merupakan suatu program jahat (Hidayatulloh, 2014). Ancaman *malware* dan penyebarannya bisa melalui berbagai cara. Salah satu cara yang sering dilakukan untuk menyebarkan *malware* dengan cara menyisipkannya di sebuah aplikasi ataupun file tertentu (Cakrawala, 2021).

Dengan migrasi antivirus yang dilakukan pada penelitian ini diharapkan dapat menghasilkan data temuan kejahatan *cybercrime* berupa *malware* yang masuk ke ruang lingkup jaringan berhasil di *cleaned*, *quarantine* bahkan langsung di *blocked* secara otomatis.

Dengan Migrasi, maka dapat melakukan pencegahan dengan terkelola sehingga dapat membantu tim keamanan dan IT Infrastruktur Jaringan. Dengan memperbaharui *Simple Network Time Protocol* dapat memberikan dukungan dan pemantauan secara multiregional sepanjang waktu, serta merespon ancaman secara langsung bila diperlukan (Sitompul, 2021).

Hal ini juga bermanfaat dalam meng-atasi kendala yang terkait dengan kinerja di lingkungan jaringan, menjamin ketersediaan sumber daya, menjamin keamanan, men-yediakan layanan-layanan yang mendukung pekerjaan selama *Work From Home (WFH)* Pengguna layanan dalam system jaringan serta aplikasi-aplikasi yang terkait dengan komputasi ini sangat membutuhkan kinerja tinggi (Yuliandoko, 2018), karena hal inilah yang paling diinginkan untuk membantu kinerja yang membutuhkan teknologi layanan jaringan yang aman disaat melakukan *transfers* data dan pertukaran informasi melalui media jaringan.

Cara yang paling mudah untuk membatasi akses adalah dengan mengharuskan pengguna untuk mengotentikasi dirinya sebelum memberikannya akses, tetapi tetap saja banyak kasus serangan yang dilaporkan. Pada umumnya langkah pertama yang dilakukan penyerang adalah mencari infor-masi lengkap tentang korbannya, seperti layanan yang berjalan, *port* yang terbuka dan versi dari *software* untuk menemukan kelemahan yang belum di *Patch* bahkan *Zero-Day* (Ablon dan Bogart, 2017).

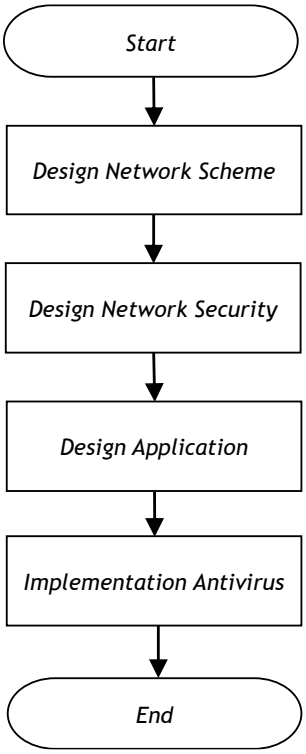
Berdasarkan latar belakang masalah yang sudah disampaikan, maka dalam tulisan ini akan menjelaskan bagaimana cara melakukan konfigrasi dan mengimplementasikan *trend micro-Antivirus client*, baik untuk PC, *notebook* ataupun server pada infrastruktur jaringan.

Selain hal tersebut, tulisan ini juga menjelaskan bagaimana melindungi jaringan dari gangguan *cybercrime* termasuk *virus worm, Trojan, malware, spyware*, *phishing*, serta bagaimana cara menscan *system* jaringan dari *server* pusat (Adenansi dan Novarina, 2017).

Penelitian yang dilakukan bertujuan untuk mengimplementasi antivirus *client server* yang dapat melakukan *scan* di setiap *client* yang terhubung jaringan local secara maupun terpusat juga meng*update* secara terpusat, mendeteksi jenis serangan yang sering terdapat *system* jaringan.

2. METODOLOGI

Dalam pelaksanaan penelitian yang dilakukan terdapat beberapa tahap, yaitu *design network scheme*, *design network security*, *design application* dilanjutkan *implementation antivirus* seperti pada Gambar 1.



Gambar 1. Alur pelaksanaan penelitian

2.1. *Design Network Scheme*

Sebagai upaya untuk melihat detail topologi jaringan maka perlu di revitalisasi *Design Network Scheme* pada PT Retail Group Indonesia. Hasil rancangan ini akan menjadi acuan dalam membuat topologi jaringan sebagai analisa kebutuhan yang dalam mendukung penelitian ini.

2.2. *Design Network Security*

Untuk memperkuat keamanan dari berbagi tindak kejahatah digital, maka *Design Network Security* perlu diterapkan dalam Infrastruktur PT Retail Group Indonesia sesuai yang dibutuhkan perusahaan (Haryanto dan Adhipta, 2016).

2.3. *Design Application*

Perlu dikembangkan penggunaan *Design Application* yang *support* dengan *system* keamanan jaringan salah satunya dengan menerapkan perangkat lunak *antivirus* Tren Micro dengan melakukan Migrasi *software* lama untuk *system* keamanan beraktifitas didalam jaringan (Bilah dan Infantono, 2019).

2.4. *Netwok Testing*

Dalam melakukan pengujian dilakukan untuk beberapa *client* yang terhubung di dalam baik yang menggunalkan system operasi yang beragam mulai dari Windows 8, Windows 10, SQL *server* 2008. Pengujian dilakukan dalam rangka untuk melihat bagaimana kondisi jaringan ini sudah layak uji dan mampu mendukung kinerja keamanan jaringan seperti harapan user (Wijaya dan Panca, 2020).

2.5. *Implementation Antivirus*

Seluruh user yang berada diruang lingkup infrastruktur dan sudah *joint* domain harus diinstal *antivirus tend micro* sebagai upaya mendektesi *malware* yang menyusup ke dalam jaringan melalui aktivitas user ke internet.

3. HASIL DAN PEMBAHASAN

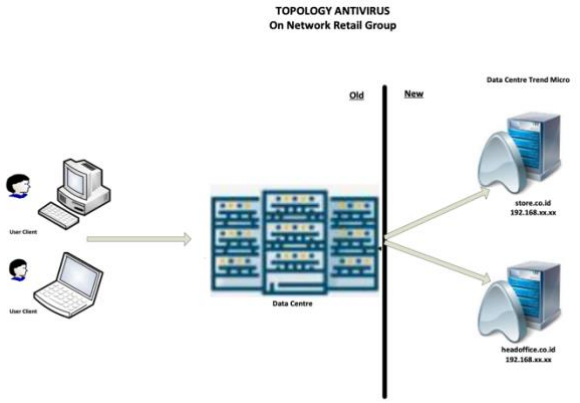
3.1. Usulan Topologi Jaringan

Dalam penerapan jaringan, karena topologi yang akan dibangun ini terhubung langsung antara *local area network* (pusat) dengan *local area network* cabang yang berada ruang lingkup data center dimana router akan digunakan sebagai lalulintas jaringan luar menuju *data center*, fasilitas yang akan dibangun menggunakan *Forticlient VPN*, jaringan luar bisa diakses Ketika karyawan /*user* tidak bekerja diruang lingkup kantor *Work From Fome* (WFH) sebagai *client*. Sebagai salah satu pening-katan keamanan maka perlu penerapan migrasi *anti virus* terbarukan sebagai salah satu bagian infrastruktur *Simple Network Time Protocol (SNTP)*. Adapun *topology* yang diusulan seperti pada Gambar 2.

3.2. Penerapan Keamanan Jaringan

Perangkat perangkat yang dipasang dan dikonfugurasi sebagai *gateway* lalu lintas keluar masuk data didalam infrastrktur adalah *router mikrotik* yang memiliki dua *fitur* yang ada di

firewall, yaitu *Network Address Translation* (NAT) dan *filtering*.



Gambar 2. *New topology antivirus*

3.2.1. *Network Address Translation (NAT)*

NAT menjadi protokol dalam suatu sistem jaringan yang menghubungkan antara jaringan *internal* dengan jaringan eksternal melalui perangkat keras, dimana *router* yang akan dikonfigurasi dan bisa berfungsi sebagai *firewall* yang memiliki peranan dalam merubah alamat pengirim dalam format yang berbeda hal ini untuk melihat apakah pakaet data tersebut bersumber dari luar jaringan atau masih dalam ruang lingkup jaringan yang sama, karena cara kerja NAT mampu mengubah paket data yang berasal dari PC/laptop *client* yang akan lalu lalang di jaringan.

Router ini menjadi piranti ke 3 yang akan dikofigurasi sebagai NAT untuk membantu menjalankan komunikasi dengan tugas melakukan penyamaran, tujuan penyamaran ini adalah untuk kebutuhan pengubahan data dari PC/laptop *client* yang akan melewati *gateway*. Penyamaran diletakan jalur keluar masuk paket data di jaringan ini berfungsi untuk melindungi *IP Client* agar tidak mudah di *hack* saat berada di jaringan *public* ,metode penyamaran ini akan menyem-bunyikan PC/laptop *client* yang ada dijaringan lokal sekaligus membuat PC dan laptop *client* tersebut terlindungi ke IP *Address router*.

3.2.2. *Filtering*

Keamanan jaringan yang menjadi salah satu aktivitas berbahaya harus ditingkatkan dengan cara memfungsikan PPTP (*Point-to-Point Tunneling Protocol*) sebagai *filtering* di *server*. Jika PPTP *filtering* difungsikan dengan baik, maka metode ini sangat luwes dan fleksibel dalam mendukung *protocol layer* dalam hal pengiriman dan penrimaan paket data menuju semua *client* yang tervalidasi atau sah. Hal ini sangat membantu, mencegah semua paket yang tidak sah menembus jaringan karena *protocol* ini akan membuka link dan membentuk sesi dengan saling bertukar informasi. Begitu juga untuk pemakaian enkripsi PPTP, PPTP *filtering* melindugi agar data yang terenkripsi dan terverifikasi bisa berlalu lalang ke dalam jaringan pribadi dengan jaringan perusahaan melalui *gateway yang* dibangun untuk melakukan testing lintasan dan persetujuan untuk penggunaan lintasan tersebut.

3.3. *Design Application* (Rancangan Aplikasi)

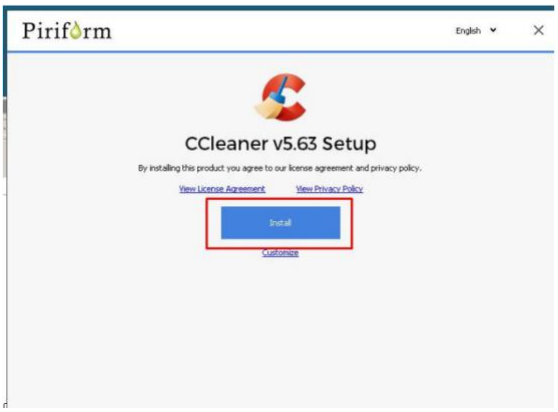
Sebagai upaya meningkatan keamanan dijaringan perusahaan dan memberikan kenyaman disaat melaukan aktivitas komunikasi di jaringan *Internet*, maka perlu dilakukan *migrasi software sophos* ke *trend Micro* seperti pada Gambar 3.

Gambar 3. Antivirus Trend Micro

Ketika akan mengimplementasikan *antivirus* sebagai langkah menerapkan keamanan dari tindak kejahatan yang akan menyusupi *system*, dimana *antivirus* yang digunakan sebelum sudah tidak mampu lagi mendukung kinerja keamanan jaringan dalam menditeksi penyerang atau tindak kejahatan yang terjadi didalam aktifitas jaringan, hal yang penting untuk diketahui adalah adanya suatu keseimbangan antara mengamankan data dari user untuk diverifikasi oleh *antivirus* dari seluruh aktifitas yang terhubung ke jaringan luar agar dapat masuk ke dalam jaringan *internal*. Maka dari itu, hal yang perlu dilakukan adalah dengan melakukan analisis resiko pada jaringan, menentukan *level* keamanan yang diperlukan pada suatu organisasi, serta melakukan identifikasi terhadap informasi-informasi yang perlu untuk dilindungi dari berbagai tindakan serangan pada jaringan.

Hal ini sangat penting untuk menentukan cara terbaik implementasi kebijakan keamanan pada suatu organisasi atau perusahaan yang sudah ada dan memastikan tidak terjadi masalah baik dari sisi manajemenl maupun teknis. Cara yang terbaik adalah dengan mengimplementasi *antivirus* yang mendukung dengan kondisi sistem operasi yang digunakan *user* dalam berinteraksi dengan jaringan luar dan di verifikasi kepentingannya serta memastikan bahwa *user* yang melakukan akses terhadap suatu sumber daya secara aman dan efisien. Untuk implementasi kebijakan keamanan dengan migrasi *antivirus* yang mampu mendukung peningkatan keamanan jaringan.

Untuk melakukan migrasi *antivirus* lama menjadi antivirus terbaru, dalam penelitian ini menggunakan antivirus *trend micro*. Adapun yang harus dilakukan adalah mempersiapkan aplikasi *seperti CCsetup563.exe Revo-Uninstaller_Portable*. Setelah itu harus Instal *CCleaner V5.63 Setup* sebagai upaya menerapkan sistem keamanan yang lebih handal dalam mendektsi serangan yang datang dari jaringan luar (lihat Gambar 4). Berikut adalah tahapan untuk migrasi sebelum implementasi *software antivirus* baru.

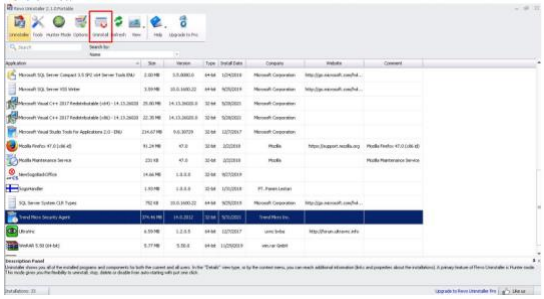


Gambar 4. *Setup* CCleaner V5.63

Setup CCleaner ini berfungsi untuk membersihkan *cache* pada PC atau laptop agar dapat bekerja secara optimal. *CCleaner* mampu untuk membersihkan *internet cache, internet history, download history* yang merupakan celah yang disusupi penyerang.

Setelah semua langkah-langkah seperti *Custom Clean, Custom Clean, Custom Clean, Registry, Scan for Isuse*, dijalankan maka akan muncul tahap finish seperti pada Gambar 5. Jika prosedur konfigurasi *CCleaner V5.63* selesai hal yang harus dilakukan adalah dengan menjalakan *Revo Uninstale* seperti pada Gambar 6. Ini dilakukan untuk menghidari masalah memori perangkat penuh. Hal ini dikarenakan banyaknya aplikasi yang terpasang. Untuk meringankan memori perangkat, sebaiknya hapus beberapa aplikasi yang tidak terpakai, maka dipilih *Revo Uninstaller* untuk melakukan pelepasan aplikasi yang terpasang.

Gambar 5. *Finished setup* CCleaner V5.63

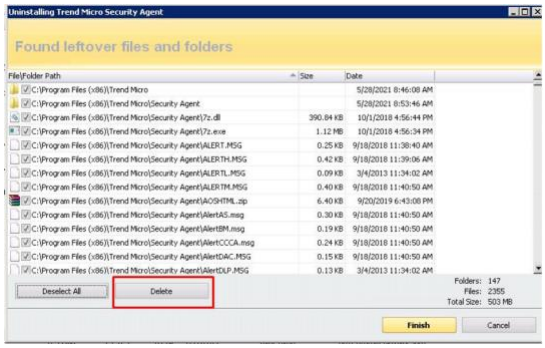


Gambar 6. *Revo Uninstaler*

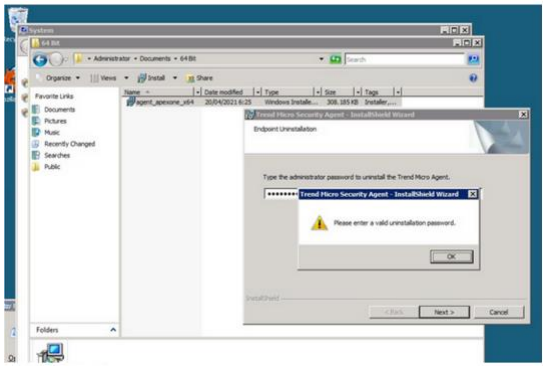
Software ini menjadi *uninstaller* yang cukup efektif untuk menghapus aplikasi berserta *file-file* yang terdapat di dalam PC atau Laptop. Sehingga seluruh bagian aplikasi yang dihapus pun tidak ada yang tertinggal dalam perangkat. Revo ini dibuat khusus untuk windows. Tahap berikutnya adalah menjalankan Revo Unistaller dengan cara Pilih *Trend Micro Security Agent*, pilih *Uninstall*, kemudian pilih yes , pilih Trend *Micro Security Agent* pilih *Uninstal, Select All* kemudian *delete, Select All*, lalu klik *Delete*, terakhir *finish* seperti terlihat pada Gambar 7.

Berikut ini *antivirus Trend Micro* yang di implementasikan untuk mendeteksi serangan sebagai peningkatakan keamanan jaringan ketika

user melakukan aktifitas dengan jaringan luar. Pastikan *instalasi* antivirus ini sudah dijalankan dengan benar hingga *finish* (lihat Gambar 8).



Gambar 7. *Finished Revo Uninstaler*



Gambar 8. *Install Trend Micro*

Setelah semua tahapan dalam implementasi antivirus sudah dilakukan, maka perlu dilakukan pengamatan untuk memastikan bahwa *antivirus (Trend Micro*) mampu bekerja dengan baik. Cara termudah yang dapat dilakukan adalah dengan menggunakan *command ping* untuk melakukan verifikasi terhadap komunikasi.

Jika percobaan koneksi jaringan dengan menggunakan perintah ping tidak berhasil atau *time out*, maka dapat dilakukan dengan cara menghentikan *antivirus* untuk kemudian dijalankan kembali. Hal ini harus dilakukan pada semua PC atau laptop yang terhubung dalam jaringan. Pengujian serangan jaringan dilakukan dengan menscan atau *running antivirus*. Pastikan jaringan sudah terkoneksi, dalam *log* akan terlihat serangan yang menyusupi seperti Gambar 9.

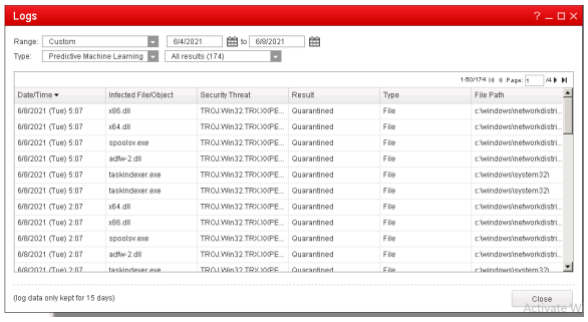
Dari pengujian *scanning* yang dilakukan dengan menggunakan *antivirus Trend micro* ini didapat ada penyerang berupa *malware Trojan* seperti pada Gambar 10 masuk ke dalam ruang lingkup jaringan LAN, hal yang harus dilakukan untuk menghetikan malware ini *cleaned* (lihat Gambar 11).

Gambar 9. Koneksi jaringan

Gambar 10. *Scan antivirus*

Gambar 11. Hasil *scan antivirus*

Pengujian terhadap serangan Malware dilakukan peneliti selama periode 6/4/2021 sampai dengan 6/8/2021 dari hasil *log* ini menjadi acuan untuk menganalisa langkah yang harus dilakukan untuk mencengah terjadi dampak yang merugikan, seperti pada Gambar 12. Bahwa *malware trojan* ini sudah harus di *quarantined* karena sudah menyusup ke dalam *file*.



Gambar 12. *Log scan antivirus*

Pengujian terhadap serangan *Malware* juga dilakukan peneliti ldiberberpa IP Addres di ruang lingkup jaringan LAN terhubung dengan jaringan luar atau Internet, seperti pada Gambar 13. Hasil log dari scanning anti virus dengan menggunakan Teend Micro, *Risk Level High*, *action* yang harus dilakukan segera *Blocked*.

Gambar 13. Log pengujian IP

Kejahatan digital atau lebih sering disebut *cybercrime* selalu mengintai aktifitasnya para pengguna komputer yang terhubung jaringan internet, sehingga mempermudah para pelaku kejahatan meskipun dengan jarak yang sangat jauh sekali (Rhode, Burnap dan Jones, 2018). Dengan perkembangan teknologi dan *software* menerapkan pergantian antivirus lama menjadi *anativirus* dengan versi terbaru yang sudah di uji ke dalam sistem mampu memproteksi serangan dengan *cleaned*, *quarantine* bahkan langsung di *blocked* secara otomatis.

4. SIMPULAN

Berdasarkan data yang didapatkan mengenai *protocol* jaringan hasil dari *scanning antivirus* menggunakan Trend Micro adalah antivirus untuk scanning malware mudah dibandingkan dengan aplikasi seperti *forensic tools snort* karena memerlukan penyetingan pada *snort.conf* sementara pada antivirus *trend micro* ini hanya cukup memilih menjalankan *scanning* hal ini bisa dilakukan oleh *user* ataupun *administrator* secara langsung. Sehingga administrator jaringan dapat meng-analisa paket jaringan yang sedang berlangsung.

Pengetahuan tentang *malware* juga diperlukan untuk antisipasi penyebaran *malware* yang semakin kompleks dengan berbagai macam cara. *Analysis malware* digunakan untuk mendeteksi *malware* terhadap suatu program yang terindikasi terkena *malware*. Pada *malware dynamic* terdapat beberapa *tools* yang dapat digu-nakan dan menambah pengetahuan penting bagi para pengguna jejaringan social atau internet. Diharapkan implementasi ini dapat melindungi seluruh komputer *client* dari segala serangan (*malware, virus, worm, Trojan*) yang terdapat pada jaringan.

UCAPAN TERIMA KASIH

Dalam kesempatan ini peneliti menyampaikan banyak terima kasih kepada LPPM Universitas Pakuan yang sudah memberikan pendanaan dalam bentuk hibah penelitian.

DAFTAR PUSTAKA

Ablon, L. dan Bogart, A. (2017) *Zero days, thousands of nights: The life and times of zero-day vulnerabilities and their exploits*. 1st edn. California: Rand Corporation [Cetak].

Adenansi, R. dan Novarina, L.A. (2017) 'Malware dynamic', *JoEICT (Journal of Education And ICT)*, 1(1), hal. 37–43.

Adnan, M.S., Ikhwan, S. dan Rahmawati, Y. (2018) 'Implementasi Load Balancing Metode ECMP, NTH dan PCC dengan Empat Link Internet Menggunakan Mikrotik', in *Proceedings on Conference on Electrical Engineering, Telematics, Industrial Technology, and Creative Media. Conference on Electrical Engineering, Telematics, Industrial technology, and Creative Media (CENTIVE)*,

Purwokerto: Institut Teknologi Telkom Purwokerto, hal. 308–314.

Bilah, C.O. dan Infantono, A. (2019) 'Pengembangan Aplikasi Mobile Kamus Istilah Aeronautika pada Platform Android Sesuai Standar ISO 25010', in *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO). Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU)*, Jakarta: Akademi Angkatan Udara, hal. 195–202.

BSSN, - Badan Siber dan Sandi Negara (2022) *Laporan Tahunan Monitoring Keamanan Siber Tahun 2021*. Jakarta: Badan Siber dan Sandi Negara.

Cakrawala (2021) 'Apa Itu Cyber Security? Mengapa Cyber Security Kini Makin Penting?', *Info Komputer*, hal. 1–2.

Haryanto, E. dan Adhipta, D. (2016) 'Meningkatkan Mekanisme Keamanan Otorisasi Port Dengan Metode Simple Port Knocking Tunneling', in *Prosiding Konferensi Nasional Penelitian Matematika dan Pembelajarannya (KNPMP I). Konferensi Nasional Penelitian Matematika dan Pembelajarannya (KNPMP I)*, Surakarta: Universitas Muhammadiyah Surakarta, hal. 827–834.

Hidayatulloh, S. (2014) 'Analisis dan Optimalisasi Keamanan Jaringan Menggunakan Protokol IPSec', *Jurnal Informatika*, 1(2), hal. 93–104.

Rhode, M., Burnap, P. dan Jones, K. (2018) 'Early-stage malware prediction using recurrent neural networks', *Computers & Security*, 77, hal. 578–594.

Sitompul, J. (2021) *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. 1st edn. Jakarta: Tatanusa [Cetak].

Wijaya, N.H. dan Panca, B.S. (2020) 'Analisis Litensi Metode PCC, NTH dan ECMP untuk Load Balance dan Failover', *Jurnal STRATEGI - Jurnal Maranatha*, 2(1), hal. 177–189.

Yuliandoko, H. (2018) *Jaringan Komputer Wire dan Wireless Beserta Penerapannya*. 1st edn. Yogyakarta: Deepublish [Cetak].